日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１２月２５日

出 願 番 号
Application Number: 特願２００２－３７４７２１

[ST. 10/C]: [ＪＰ２００２－３７４７２１]

出 願 人
Applicant(s): カシオ計算機株式会社

２００３年１１月 ６日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０９１７６１

【書類名】　特許願
【整理番号】　02-1507-00
【提出日】　平成14年12月25日
【あて先】　特許庁長官　殿
【国際特許分類】　G06T　1/00
G06K　9/00
【発明者】
【住所又は居所】　東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社　羽村技術センター内
【氏名】　喜多　一記
【特許出願人】
【識別番号】　000001443
【氏名又は名称】　カシオ計算機株式会社
【代理人】
【識別番号】　100090033
【弁理士】
【氏名又は名称】　荒船　博司
【選任した代理人】
【識別番号】　100093045
【弁理士】
【氏名又は名称】　荒船　良男
【手数料の表示】
【予納台帳番号】　027188
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　カード型デバイスおよび認証システム

【特許請求の範囲】

【請求項１】　電子機器と接続端子を介して接続されるカード型デバイスであって、

接続端子を有するカード型の筐体と、

この筐体の端面にその外周面が突出して設けられた回転ローラと、

この回転ローラの外周面に当接される指の一次元指紋データを取得する一次元指紋データ取得部と、

前記回転ローラを回転させることにより、前記一次元指紋データ取得部により位置を連続的に変えて取得される一次元指紋データから二次元像としての指紋データを合成する指紋データ合成部と、

前記電子機器との間でデータの授受を行うインターフェース部と、

を備えたことを特徴とするカード型デバイス。

【請求項２】　請求項１に記載のカード型デバイスにおいて、

前記筐体は、前記接続端子が配されるとともに前記電子機器に設けられたカード・スロットに挿入される挿入部を備え、前記回転ローラはこのカード・スロットの挿入口から露出する端面に設けられることを特徴とするカード型デバイス。

【請求項３】　請求項１または２に記載のカード型デバイスにおいて、

前記指紋データを、当該カード型デバイスに固有であり、かつ、対となる公開復号鍵によってのみ復号化することができる秘密暗号鍵により暗号化する暗号化手段を備えたことを特徴とするカード型デバイス。

【請求項４】　請求項１または２に記載のカード型デバイスにおいて、

前記指紋データ合成部により合成された指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、前記インターフェース部における前記電子機器との間のデータの授受を制限する制御部を備えたことを特徴とするカード型デバイス。

【請求項５】　電子機器と、請求項１または２に記載のカード型デバイスとが接続されてなる認証システムであって、

前記電子機器は、前記カード型デバイスから送信される指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、当該電子機器の動作を制限する制御部を備えたことを特徴とする認証システム。

【請求項６】　電子機器と、請求項３に記載のカード型デバイスとが接続されてなる認証システムであって、

前記電子機器は、前記カード型デバイスから送信される暗号化された指紋データを前記公開復号鍵により復号化し、復号化された指紋データと予め登録された指紋データとの一致を照合し、両指紋データが一致しない判断した場合、当該電子機器の動作を制限する制御部を備えたことを特徴とする認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、カード型デバイスおよび認証システムに関する。

【０００２】

【従来の技術】

近年、電子機器のネットワーク化が進み、電子機器間の通信が自由になり、どこからでも様々な情報にアクセスできるようになってきている。それに伴い他者の不正アクセスを防止するためにセキュリティの重要性が高まっている。セキュリティ技術の一つに指紋によってユーザを認証する方法があり、指紋読取センサをＰＣカードに設けたものがある。

【０００３】

例えば、ＣＣＤ（Couple charged Device）等から成る指紋読取センサをＰＣカードの把持位置に設けたものがある（特許文献１参照）。このＰＣカードを把持すると、自動的に指紋が採取され、指紋に基づいて使用者の認証が行われ、ＰＣカードに記憶された個人情報等へのアクセスが防止されるようになっている。

【０００４】

他の例として、ＰＣカードの挿入部に指紋読取センサを備えた指紋読取センサを相対回転可能に機械的に連結したものもある（例えば、特許文献２参照）。

このＰＣカードを電子機器のカード・スロットに装着させることにより、本人

を認証するための認証装置として使用することができ、認証されない場合は電子機器の動作が制限されたり、ＰＣカードへのアクセスが禁止される。

【０００５】

【特許文献１】

特開２０００－４８１７７号公報

【特許文献２】

特開２００１－２３３３４４号公報

【０００６】

【発明が解決しようとする課題】

しかしながら、特許文献１に記載の指紋読取センサは把持位置に設けられているので、ＰＣカードを電子機器のカード・スロットに装着すると指紋読取センサがカード・スロットの内部に配されてしまい、ＰＣカードを電子機器に装着した状態でユーザを認証することはできなかった。

一方、特許文献２に記載の指紋読取センサは、ＰＣカードを電子機器のＰＣカードスロットに装着させたときに大きく外部へ突出してしまうので、この指紋読取センサ付きのＰＣカードを電子機器に装着させたままで携帯させにくいという問題があった。

【０００７】

また、両指紋読取センサは、指を載置可能な平面矩形状に形成されており、ＣＣＤなどの高価な半導体素子を用いるためコスト高となる。さらに、二次元ＣＣＤチップは実装面積を要することから、携帯電話やＰＤＡ（Personal Digital Assistance）等の拡張メモリとして使用されるＣＦカード（Compact Flash Card）、ＳＤカード（Secure Digital Card）、ＭＭＣ（Multi Media Card）カード、ＵＳＢ接続携帯型フラッシュメモリ等の超小型のメモリカードに指紋読取センサを設けることはできなかった。このため、指紋認証によりこれらのメモリカードに記憶された情報を保護したり、携帯電話やＰＤＡ等にメモリカード等により指紋認証機能を拡張させることができなかった。

【０００８】

本発明の課題は、指紋読取センサを搭載した超小型のカード型デバイスおよび

このカード型デバイスを用いた認証システムを提供することである。

【０００９】

【課題を解決するための手段】

上記課題を解決するために、請求項１に記載の発明は、電子機器と接続端子を介して接続されるカード型デバイスであって、接続端子を有するカード型の筐体と、この筐体の端面にその外周面が突出して設けられた回転ローラと、この回転ローラの外周面に当接される指の一次元指紋データを取得する一次元指紋データ取得部と、前記回転ローラを回転させることにより、前記一次元指紋データ取得部により位置を連続的に変えて取得される一次元指紋データから二次元像としての指紋データを合成する指紋データ合成部と、前記電子機器との間でデータの授受を行うインターフェース部と、を備えたことを特徴とする。

【００１０】

請求項１に記載の発明によれば、一次元指紋読取センサにより指紋の二次元像を得ることとしたので、指紋読取センサを実装するための面積も小さくすることができ、ＣＦカード等の超小型のメモリカードにも指紋読センサ設けることができる。また、二次元の指紋読取センサを設ける場合に比べて、指紋センサを構成する部品コストを低減することができる。これらにより、携帯電話やＰＤＡ等の一般ユーザ向けの携帯用電子機器にも容易に指紋認証機能を拡張させることができる。

【００１１】

さらに指を回転ローラに当接させた状態で回転させることにより、指を一次元指紋読取センサに対して移動させることができるので、指の変形やゆがみを防止した状態で一次元指紋読取センサに指紋を読み取らせることができ、操作性に優れている。

【００１２】

請求項２に記載の発明は、請求項１に記載のカード型デバイスにおいて、前記筐体は、前記接続端子が配されるとともに前記電子機器に設けられたカード・スロットに挿入される挿入部を備え、前記回転ローラはこのカード・スロットの挿入口から露出する端面に設けられることを特徴とする。

【００１３】

請求項２に記載の発明によれば、回転ローラはカード・スロットの挿入口から露出する端面に設けられるので、カード型デバイスを装着させた状態でカード・スロットから指紋読取センサが大きく突出することがなく、携帯性に優れている。また、ユーザは、カード・スロットの挿入口に直交するように指をスライドさせればよいので、操作性に優れている。

【００１４】

請求項３に記載の発明は、請求項１または２に記載のカード型デバイスにおいて、前記指紋データを、当該カード型デバイスに固有であり、かつ、対となる公開復号鍵によってのみ復号化することができる秘密暗号鍵により暗号化する暗号化手段を備えたことを特徴とする。

【００１５】

請求項３に記載の発明によれば、暗号化手段により指紋データを秘密暗号鍵により暗号化するので、暗号化された指紋データはこの秘密暗号鍵と対となる公開復号鍵を有するものにしか復号化することができず、指紋データの悪用を防ぎ、セキュリティをより高めることができる。

【００１６】

請求項４に記載の発明は、請求項１または２に記載のカード型デバイスにおいて、前記指紋データ合成部により合成された指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、前記インターフェース部における前記電子機器との間のデータの授受を制限する制御部を備えたことを特徴とする。

【００１７】

請求項４に記載の発明によれば、カード型デバイスを電子機器に接続する前に指紋に基づいてユーザを認証することできる。また、一次元指紋読取センサを介して取得された指紋データが、予め登録された指紋データと一致しない場合は、電子機器との間のデータの授受が制限されるので、カード型デバイスの不正使用およびカード型デバイスへの不正アクセスを防止することができる。

【００１８】

請求項５に記載の発明は、電子機器と、請求項１または２に記載のカード型デバイスとが接続されてなる認証システムであって、前記電子機器は、前記カード型デバイスから送信される指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、当該電子機器の動作を制限する制御部を備えたことを特徴とする。

【００１９】

請求項５に記載の発明によれば、電子機器はカード型デバイスから送信される指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、制御部は電子機器の動作を制限するので、電子機器およびカード型デバイスの不正使用およびカード型デバイスへの不正アクセスを防止することができる。

【００２０】

請求項６に記載の発明は、電子機器と、請求項３に記載のカード型デバイスとが接続されてなる認証システムであって、前記電子機器は、前記カード型デバイスから送信される暗号化された指紋データを前記公開復号鍵により復号化し、復号化された指紋データと予め登録された指紋データとの一致を照合し、両指紋データが一致しない判断した場合、当該電子機器の動作を制限する制御部を備えたことを特徴とする。

【００２１】

請求項６に記載の発明によれば、カード型デバイスにより暗号化された指紋データは、この秘密暗号鍵と対となる公開復号鍵に基づいて復号化可能な電子機器でしか指紋データを照合することができないので、よりセキュリティを向上することができる。

【００２２】

【発明の実施の形態】

以下、図面を参照して本発明に係る第１の実施の形態～第４の実施の形態を説明する。

【００２３】

〔第１の実施の形態〕

本発明に係る第１の実施の形態を説明する。

まず、構成を説明する。図１（ａ）、（ｂ）、（ｃ）に本実施の形態のカード型デバイスの外観構成例を示す。カード型デバイス１は、所定記憶容量の記憶媒体（図示略）を有し、電子機器に設けられるカード・スロットに挿入されて使用されるものであり、例えば、ＰＣカード、ＣＦカード、ＭＭＣカード、ＳＤカード、メモリスティック（登録商標）等の規格化されたメモリカードを挙げることができる。

【００２４】

カード型デバイス１の筐体１０は、カード・スロットの一端部１１には指紋読取部２が設けられ、他端部１２の背面１２ａには電子機器と電気的に接続するための接続端子１３が設けられている。また、カード型デバイス１は、その筐体１０の他端部１２側はカード・スロットに挿入される挿入部となっており、指紋読取部２を設けた一端部１１はカード・スロットから露出するようになっている。

【００２５】

図２に示すようにカード型デバイス１は、その機能的構成として、指紋読取部２および接続端子１３の他に、信号処理部１４、メモリ１５、制御部16、入出力Ｉ／Ｆ部１７を備えている。これら各構成要素はバス１８で接続されている。

【００２６】

指紋読取部２は、図３に示すように、回転ローラ２１、光源２２、セルフォックレンズアレイ２３、基板２４、一次元指紋読取センサ２５を含み、回転ローラ２１の外周面２１ａの一部が筐体の一端面１１ａに設けられたスリット１１ｂから外部に突出している。

【００２７】

回転ローラ２１は円筒状を呈しており、アクリル樹脂、ポリカーボネイト、ホウケイ酸ガラス、石英ガラス等の透光性材料から構成される。スリット１１ｂから露出した回転ローラ２１の外周面２１ａに指１００を圧接させて、その状態で指１００を所定の方向に移動させると、回転ローラ２１が回転する。

【００２８】

回転ローラ２１には指紋読取部２と制御部１６との接続をＯＮ／ＯＦＦするマ

イクロスイッチ１９（図２参照）と、回転ローラ２１が所定角度回転する毎にパルス信号を発生して制御部１６に出力するロータリーエンコーダ（図示略）が設けられている。マイクロスイッチ１９は回転ローラ２１の外周面２１ａに指１００が圧接されるとＯＮになり、指が離されるとＯＦＦになる。

【００２９】

なお、ロータリーエンコーダの代わりに、回転ローラ２１の外周面２１ａに回転量検出のための所定の印刷パターンを印刷しておき、そのパターンを読み取って制御部１６にパルス信号を出力する回転検知センサを設けてもよい。

【００３０】

図２および図３に示すように、回転ローラ２１は中空に形成されており、その内部に光源２２、セルフォックレンズアレイ２３、基板２４、一次元指紋読取センサ２５及びこれらの部品を保持するホルダ２６が設けられている。ホルダ２６は、回転ローラ２１の一方の端又は両端から延出して筐体１０に固定されており、回転ローラ２１が回転してもホルダ２６は回転しない状態に筐体１０に支持されている。

【００３１】

光源２２は、スリット１１ｂに向けて光を発することで回転ローラ２１の外周面２１ａに当接した指１００に指紋読取光L_0を照射するものであり、ＬＥＤ、有機ＥＬ、無機ＥＬ及び蛍光管等といった自発光素子から構成される。

【００３２】

セルフォックレンズアレイ２３は、回転ローラ２１の軸心に対して直交する中心軸を有する複数のセルフォックレンズを回転ローラ２１の軸心に平行な列を成すように配列したものであり、回転ローラ２１の外周面２１ａに当接する指１００の一次元像を一次元指紋読取センサ２５に結像させるものである。セルフォックレンズアレイ２３の光軸は、回転ローラ２１の軸心に対して直交し、セルフォックレンズアレイ２３の入射面２３ａはスリット１１ｂに指向している。

【００３３】

なお、セルフォックレンズは円柱状のロッドレンズであり、中心軸から周面にかけて放物線状の屈折率分布を有し、中心軸において屈折率が最も高く、周面に

おいて屈折率が最も低い自己収束型のレンズである。それぞれのセルフォックレンズは球面レンズと光学的にほぼ等価な作用を有し、これら全てのセルフォックレンズは互いに光学的に等価な性質を有している。

【００３４】

セルフォックレンズアレイ２３が一次元指紋読取センサ２５の受光面２５ａに結像する指１００の一次元像は、回転ローラ２１の外周面２１ａに当接された指１００の一次元像と向きが等しく（反転されず）、等倍になる。

【００３５】

基板２４は、一次元指紋読取センサ２５を表面に実装するとともに、信号処理部１４と制御部１６と信号の送受を行うための配線が施されている。

【００３６】

一次元指紋読取センサ２５は、リニア型ＣＣＤイメージセンサ、リニア型ＣＭＯＳイメージセンサ等の光電変換素子で構成され、その受光面２５ａはスリット１１ｂに対向するように、回転ローラ２１の軸心に沿って平行に設けられている。セルフォックレンズアレイ２３等により受光面２５ａに結像された指紋の一次元像を電気信号としての一次元指紋信号に変換する。

【００３７】

信号処理部１４は、アナログ信号である一次元指紋信号をデジタル信号に変換して一次元指紋データを生成し、制御部１６を介してメモリ１５に出力する。

【００３８】

制御部１６は、ＣＰＵ（Central Processing Unit）、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等を備え、ＲＡＭまたはＲＯＭに記憶された指紋読取プログラム等の指定されたプログラムをＲＡＭの所定領域に展開し、これらのプログラムに基づく指紋読取処理等の各種処理を実行する。

【００３９】

指紋読取処理はマイクロスイッチ１９がＯＮすることにより開始される。ユーザが回転ローラ２１の外周面２１ａに指１００を圧接させた状態で一方向に移動させると、回転ローラ２１が回転する。このとき、マイクロスイッチ１９はＯＮになり、ロータリーエンコーダから回転ローラ２１の所定角度回転する毎にパル

ス信号が発生される。光源２２は指１００に対して指紋読取光Ｌ$_0$を照射する。指１００に反射した光Ｌはセルフォックレンズアレイ２３等により一次元指紋読取センサ２５の受光面２５ａに集光される。一次元指紋読取センサ２５は、パルス信号に同期して一次元指紋信号を生成し、信号処理部１４に出力する。信号処理部１４では、パルス信号に同期して順次入力される一次元指紋信号をＡ／Ｄ変換して一次元指紋データを生成し、メモリ１５に出力する。制御部１６は、メモリ１５に格納された一次元指紋データから、回転ローラ２１の回転方向に基づいて指紋の二次元像としての指紋データを合成する。

【００４０】

生成された指紋データは、入出力Ｉ／Ｆ部１７、接続端子１３を介して電子機器に送信される。なお、入出力Ｉ／Ｆ部１７は、電子機器との間で指紋データを含む種々のデータを所定のデータ伝送方式に従って伝送するものである。

【００４１】

次に、図４～図８を参照して、上記カード型デバイス１が装着される電子機器３（３ａ～３ｅ）について説明する。電子機器３は、カード型デバイス１が装着されることにより指紋に基づくユーザの認証を行うことができる。

【００４２】

図４に示すように、電子機器３は、カード・スロット３１、操作入力部３２、表示部３３、音声入出力部４０、移動体通信部５０、本体機能制御部６０等を備え、これらはバス３４により互いに接続される。電子機器３は、外部との無線通信機能、住所録機能、スケジュール管理機能等各種の機能を備えるもので、これらの機能の一部または全てをユーザの認証結果に基づいて制限することができる。

【００４３】

また、これらの電子機器３は、カード型デバイス１を装着することにより、ＷＥＢサイトへのアクセス認証やインターネット等のネットワークを介して行われる電子商標取引等における電子決済の際の本人認証装置として使用することもできる。

【００４４】

このような電子機器３として、例えば、図５（ａ）、（ｂ）に示す携帯電話３ａ、３ｂ、図６に示す折り畳み式携帯電話３ｃ、図７に示すＰＤＡ等の携帯型情報機器３ｄ、図８に示す腕時計等の身体装着型電子機器３ｅ等を挙げることができる。

【００４５】

図５～図８に示すように、これらの電子機器３ａ～３ｅに設けられるカード・スロット３１の位置は限定されるものではなく、カード型デバイス１を装着させたとき、指紋読取部２の回転ローラ２１を指で圧接しながら回転させることができるようになっている。

【００４６】

カード・スロット３１は接続コネクタ３１ａを備え、このカード・スロット３１にカード型デバイス１が挿入されて、接続端子１３と接続されることにより、カード型デバイス１と電子機器３とが互いに電気的に接続される。

【００４７】

操作入力部３２は、テンキー、各種機能スイッチ等を備え、そのキー操作による押下信号をＣＰＵ６１に出力する。

【００４８】

表示部３３は、ＬＣＤ（Liquid Crystal Display）等からなる表示画面を備え、ＣＰＵ６１から入力される表示情報に基づく表示を行う。

【００４９】

音声入出力部４０は、マイク４１と、スピーカ４２と、音声コーデック部４３とを備えて構成される。音声コーデック部４３はマイク４１から入力される音声信号（アナログ信号）をＡ／Ｄ変換器によりデジタル音声信号に変換し、移動体通信部５０に出力する。また移動体通信部５０を介して外部受信された音声信号（デジタル信号）を復号し、Ｄ／Ａ変換器によりアナログ音声信号に変換して、スピーカ４２に出力する。

【００５０】

移動体通信部５０は、無線基地局（図示せず）との間で着信・発信等に係る無線信号の送受信を行うアンテナ５１、ＲＦ／送受信部５２、加入者ＩＤ／端末Ｉ

Ｄ記憶部５３、通信制御部５４等を備え、ＣＰＵ６１から入力される指示に従って、通信制御部５４が無線基地局との間でＩＭＴ－２０００準拠の通信方式（例えば、Ｗ－ＣＤＭＡやｃｄｍａ２０００）に対応する携帯電話用の通信プロトコルを実行し、この通信方式で設定される通信チャネルにより、送受話音声の送受信やデータ通信を実行する。

【００５１】

本体機能制御部６０は、ＣＰＵ６１、ＲＡＭ６２、プログラムメモリ６３、データメモリ６４、入出力Ｉ／Ｆ部６５を備え、ＣＰＵ６１において、ＲＡＭ６２の所定領域を作業領域としてプログラムメモリ６３に記憶されている各種制御プログラムに従い、各部に制御信号を送って電子機器３の動作全般を制御する。

【００５２】

プログラムメモリ６３は、指紋照合プログラム６３ａ、声紋照合プログラム６３ｂを含むユーザ認証プログラム６３ｃを格納している。

ここで、本実施の形態においては、制御部はＣＰＵ６１において、この指紋照合プログラムに基づく指紋照合処理によりユーザ認証処理を実行する際に、マイクから入力されるユーザの音声（声紋）に基づく声紋照合処理とを併用することもできる。

【００５３】

データメモリ６４は、予め登録された正規のユーザの指紋データが格納された指紋データ格納領域６４ａと、同じく正規のユーザの声紋データが格納された声紋データ格納領域６４ｂを有している。

【００５４】

次に、ユーザ認証処理について説明する。ユーザがカード型デバイス１をカード・スロット３１に挿入すると電子機器３の本体機能制御部６０はユーザ認証プログラムを起動し、指紋照合処理を実行する。

【００５５】

指紋照合処理では、まず、表示部３３にユーザに対して回転ローラ２１に指１００を圧接させて一方向に移動させるように促す表示がされる。なお、このとき、スピーカ４２によりその旨を音声報知することとしてもよい。

【００５６】

ユーザが回転ローラ２１を指１００で回転させると、上記したとおり、カード型デバイス１の制御部１６による指紋読取処理が実行され、互いの入出力Ｉ／Ｆ部１７、６５を介してカード型デバイス１から指紋データが電子機器３に送信される。

【００５７】

指紋データを受信すると、電子機器３側の本体機能制御部６０は、ユーザの指紋データと、データメモリ６４に登録された指紋データとを照合し、両指紋データが一致するか否かを判断する。なお、このとき、それぞれの指紋データから特徴パターンを抽出して、その特徴パターンに基づいて両者を照合してもよい。また、回転ローラ２１に圧接された指１００の位置や押し付ける強さ等によって指紋データにずれが生じることが想定されるので、両者の照合率Ａを求め、求めた照合率Ａが予め定めた基準値（例えば、８５％など）以上であれば両指紋データが一致すると判断してもよい。

【００５８】

照合の結果、両指紋データが一致すると判断されると、表示部３３にその結果を表示させるとともに、声紋照合処理を開始する。

【００５９】

声紋照合処理では、マイク４１から採取されたユーザの声紋と、データメモリ６４の声紋データ格納領域６４ｂに登録された登録声紋データとが照合され、両声紋データが一致すると判断されると、ユーザが予め登録されている正規のユーザであることが認証される。

【００６０】

このユーザ認証処理によって、ユーザが正規のユーザであると認証されない場合、電子機器３の各種機能は制限されたままの状態となる。

【００６１】

なお、データメモリ６４には複数の登録者の指紋データや声紋データを格納しておくことができ、電子機器３はカード型デバイス１を装着することにより複数のユーザを認証することができる。従って、登録者毎に電子機器３において使用

できる機能と使用できない機能を設定することもできる。

【００６２】

また、ユーザの認証結果は、所定の時間、操作入力部３２からの操作が行われない場合、その認証結果を消去して初期状態にすることが望ましい。

【００６３】

以上説明したカード型デバイス１によれば、一次元指紋読取センサ２５により指紋の二次元像を得ることとしたので、この一次元指紋読取センサ２５を実装するための面積を小さくすることができ、ＣＦカード等の超小型のメモリカードにも指紋読取センサ設けることができる。また、二次元の指紋読取センサを設ける場合に比べて、ＣＣＤ等の指紋センサを構成する部品コストを低減することができる。これらにより、携帯電話３ａ、３ｂ、３ｃ、ＰＤＡ３ｄ、腕時計３ｅ等の一般ユーザ向けの電子機器３に容易に指紋認証機能を拡張させることができる。

【００６４】

さらに、一次元指紋読取センサ２５を透光性材料からなる回転ローラ２１の内側に配しているので、指１００を回転ローラ２１の外周面２１ａに圧接させた状態で移動させることにより、指１００を一次元指紋読取センサ２５に対して直交する方向に案内しながら移動させることができる。これにより、指紋読取時の指の変形やゆがみを防ぐことができる。また、ロータリーエンコーダ等により指の移動量を容易に管理することができるので、一次元指紋読取センサ２５により一次元指紋データを取得するタイミングを制御することができる。

【００６５】

また、回転ローラ２１は、カード・スロット３１の挿入口から突出した状態で設けられるので、回転させやすく操作性が高い。さらに、指紋読取部２をコンパクトに構成することができるので、カード型デバイス１を電子機器３に装着させた状態でも指紋読取部２がカード・スロット３１の外部に大きく突出せず、携帯性に優れている。

【００６６】

また、ユーザの認証結果に基づいて、電気機器３の動作を制限することができるので、電子機器３の不正利用、電子機器３に格納された個人情報等への不正ア

クセス、カード型デバイス１に記憶された個人情報等への不正アクセス等を防止することができる。

【００６７】

なお、上記実施の形態では、カード型デバイス１を電子機器３に装着させたときに、電子機器３により指紋に基づくユーザ認証処理を実行させるものとしたが、これに限定されるものではない。常に電子機器３にカード型デバイス１を装着させておき、例えば、移動体通信部５０を介してインターネット等の通信ネットワークを介して電子商取引を行うときなど、ユーザ認証が求められる場合にのみユーザ認証処理を実行させてもよい。

【００６８】

また、電子機器３においてユーザ認証処理を行わせるものとしたが、通信ネットワークに接続された他の電子機器（例えば、サーバ）によりユーザの認証を行うものとしてもよい。

【００６９】

〔第２の実施の形態〕

次に第２の実施の形態について説明する。第２の実施の形態では、指紋に基づくユーザ認証処理をカード型デバイス７において実行させることができる。なお、上記実施の形態と同様の構成については同様の符号を付してその説明を省略する。

【００７０】

図９に第２の実施の形態におけるカード型デバイス７を示す。図９に示すように、カード型デバイス７は、指紋照合プログラムを格納したプログラムメモリ７１と、正規ユーザの指紋データを格納したデータメモリ７２とを有している。

【００７１】

第２の実施の形態では、カード型デバイス７の制御部１６側で指紋照合処理に基づくユーザ認証処理が実行される。この場合、制御部１６は、プログラムメモリ７１に格納された指紋照合プログラムに従って、指紋照合処理を実行する。指紋照合処理では、指紋読取部２から得た一次元指紋データに基づいて合成した指紋データと、データメモリ７２に格納された指紋データとが照合される。両指紋

データが一致しないと判断した場合、入出力Ｉ／Ｆ部１７における電子機器３との間のデータの授受が制限される。

【００７２】

以上のカード型デバイス７は、電子機器３に接続する前に指紋に基づいてユーザを認証することが可能である。勿論、電子機器３にカード型デバイス７を装着させた状態で、指紋照合処理を実行するようにしてもよい。

【００７３】

また、一次元指紋読取センサ２５を介して取得された指紋データが、データメモリ７２に格納された指紋データと一致しない場合は、電子機器３との間のデータの授受が制限されるので、カード型デバイス７の不正使用およびカード型デバイス７への不正アクセスを防止することができる。

【００７４】

〔第３の実施の形態〕

次に、第３の実施の形態について説明する。なお、上記実施の形態と同様の構成については同様の符号を付してその説明を省略する。

【００７５】

図１０に示すように、第３の実施の形態におけるカード型デバイス８は、暗号化回路８１と、秘密鍵を記憶した秘密鍵メモリ８２とを有している。信号処理部１４、メモリ１５、制御部１６、暗号化回路８１、秘密鍵メモリ８２は、耐タンパー性の認証チップ内に集積されている。

【００７６】

耐タンパー性とは、ある程度までの物理的衝撃（不当アクセス・改鼠等）に抵抗する機能をいい、外部からの不当なアクセスに対し、物理的な仕組みによってアクセスできないようにする他、分解して解析するなどがあった場合には、チップそのものが回路的に破壊されるような、偽造・変造・改竄等を防止する手段を備えたものをいう。

【００７７】

暗号化回路８１は、秘密鍵メモリ８２に格納されたこのカード型デバイス８に固有の秘密暗号鍵に基づいて、制御部１６により合成された指紋データを暗号化

して、入出力Ｉ／Ｆ部１７を介して電子機器３に送信する。

【００７８】

ここで、秘密暗号鍵とは、いわゆる公開鍵暗号化方式（ＰＫＩ：Public Key Infrastructure）による暗号化・復号化を行うための鍵情報である。この秘密暗号鍵により暗号化された情報は、対応する公開復号鍵によってのみ復号化が可能である。

【００７９】

従って、本実施の形態によれば、暗号化回路８１により秘密暗号鍵により暗号化された指紋データを電子機器３または電子機器３を介して接続されるネットワーク上のサーバ等に送信するので、電子機器３またはネットワーク上のサーバ等はこの秘密暗号鍵と対となる公開復号鍵を有する場合しか指紋データを復号化することができない。よって、指紋データの悪用を防止することができ、セキュリティをより高めることができる。

【００８０】

〔第４の実施の形態〕

次に、第４の実施の形態について説明する。なお、上記実施の形態と同様の構成については同様の符号を付してその説明を省略する。

【００８１】

図１１に、第４の実施の形態におけるカード型デバイス９としてのＵＳＢ接続携帯型フラッシュメモリの外観構成例を（ａ）、（ｂ）、（ｃ）に示す。図１１（ａ）、（ｂ）、（ｃ）に示したＵＳＢ接続携帯型フラッシュメモリは、それぞれ筐体９０の他端部９１にＵＳＢ端子９２を備え、筐体９０の端面に指紋読取部２を備え、回転ローラ２１が端面から突出してもうけられている。また、内部にはフラッシュメモリFlash EPROM (Erasable Programmable Read Only Memory)を収容しており、外部メモリ装置として使用することができる。

【００８２】

これらのカード型デバイス９は、ＵＳＢ規格に基づいたシリアルインターフェース回路を備えた電子機器（例えば、ＰＤＡ、パーソナルコンピュータ）等に着脱することにより互いにデータの授受を行うことができる。

【００８３】

次に、カード型デバイス９の機能的構成を説明する。図１２に示すように、カード型デバイス９は、ＵＳＢ接続端子９２と、ＵＳＢ入出力Ｉ／Ｆ回路９３と、暗号化回路８１と、秘密鍵を記憶した秘密鍵メモリ８２と、信号処理部１４、メモリ１５、制御部１６、指紋読取部２を有している。第３の実施の形態と同様に、信号処理部１４、メモリ１５、制御部１６、暗号化回路８１、秘密鍵メモリ８２は耐タンパー性の認証チップに集積されている。

【００８４】

このカード型デバイス９は、公開鍵暗号方式に基づく電子証明書、パスワード等をフラッシュメモリに格納しておき、ＵＳＢ端子９２を介して接続された電子機器または電子機器を介してネットワーク上にトークン（Token）と呼ばれる特殊なデータで表現して送出するものである。このとき、指紋読取部２より読み取られた指紋に基づくユーザ認証が完了しない限り、電子証明書を電子機器３に送出できないように制御される。

【００８５】

ここで、指紋データの照合は第一の実施の形態と同様にカード型デバイス９が接続された電子機器側で行うものとしてもよいし、第二の実施の形態と同様にカード型デバイス９側で行うものとしてもよいし、ネットワークで接続された認証用のサーバで行うものとしてもよい。

【００８６】

また、指紋データの照合をネットワーク上の認証用のサーバで行うものとした場合、指紋データを電子機器に設けられる通信部を介して認証用のサーバに送信する際に、暗号化回路により指紋データを秘密暗号鍵に基づいて暗号化して送信してもよい。

【００８７】

これにより、電子商取引等のユーザ認証が求められる場面等で、指紋読取部２により読み取られた指紋に基づくユーザ認証が完了しない限り、個人情報である電子証明書を使用することができないので、カード型デバイス９に格納された電子証明書やパスワードなどの重要な個人情報の悪用を防ぎ、他者の「なりすまし

」等を防止することができる。

【００８８】

【発明の効果】

請求項１に記載の発明によれば、一次元指紋読取センサにより指紋の二次元像を得ることとしたので、指紋読取センサを実装するための面積も小さくすることができ、ＣＦカード等の超小型のメモリカードにも指紋読センサ設けることができる。また、二次元の指紋読取センサを設ける場合に比べて、指紋センサを構成する部品コストを低減することができる。これらにより、携帯電話やＰＤＡ等の一般ユーザ向けの携帯用電子機器にも容易に指紋認証機能を拡張させることができる。

【００８９】

さらに指を回転ローラに当接させた状態で回転させることにより、指を一次元指紋読取センサに対して移動させることができるので、指の変形やゆがみを防止した状態で一次元指紋読取センサに指紋を読み取らせることができ、操作性に優れている。

【００９０】

請求項２に記載の発明によれば、回転ローラはカード・スロットの挿入口から露出する端面に設けられるので、カード型デバイスを装着させた状態でカード・スロットから指紋読取センサが大きく突出することがなく、携帯性に優れている。また、ユーザは、カード・スロットの挿入口に直交するように指をスライドさせればよいので、操作性に優れている。

【００９１】

請求項３に記載の発明によれば、暗号化手段により指紋データを秘密暗号鍵により暗号化するので、暗号化された指紋データはこの秘密暗号鍵と対となる公開復号鍵を有するものにしか復号化することができず、指紋データの悪用を防ぎ、セキュリティをより高めることができる。

【００９２】

請求項４に記載の発明によれば、カード型デバイスを電子機器に接続する前に指紋に基づいてユーザを認証することできる。また、一次元指紋読取センサを介

して取得された指紋データが、予め登録された指紋データと一致しない場合は、電子機器との間のデータの授受が制限されるので、カード型デバイスの不正使用およびカード型デバイスへの不正アクセスを防止することができる。

【００９３】

請求項５に記載の発明によれば、電子機器はカード型デバイスから送信される指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、制御部は電子機器の動作を制限するので、電子機器およびカード型デバイスの不正使用およびカード型デバイスへの不正アクセスを防止することができる。

【００９４】

請求項６に記載の発明によれば、カード型デバイスにより暗号化された指紋データは、この秘密暗号鍵と対となる公開復号鍵に基づいて復号化可能な電子機器でしか指紋データを照合することができないので、よりセキュリティを向上することができる。

【図面の簡単な説明】

【図１】

本発明を適用した第１の実施の形態のカード型デバイスの外観構成例を示した（ａ）正面図、（ｂ）側面図、（ｃ）背面図である。

【図２】

本発明を適用した第１の実施の形態のカード型デバイスの機能的構成を示したブロック図である。

【図３】

図２に示す指紋読取部２の構成例を示した側面図である。

【図４】

本発明を適用した第１の実施の形態の電子機器の機能的構成を示したブロック図である。

【図５】

図４に示す電子機器の外観構成例（ａ）、（ｂ）を示した図である。

【図６】

図４に示す電子機器の外観構成例を示した図である。

【図７】

図４に示す電子機器の外観構成例を示した図である。

【図８】

図４に示す電子機器の外観構成例を示した図である。

【図９】

本発明を適用した第２の実施の形態のカード型デバイスの機能的構成を示した図である。

【図１０】

本発明を適用した第３の実施の形態のカード型デバイスの機能的構成を示した図である。

【図１１】

本発明を適用した第４の実施の形態のカード型デバイスの外観構成例を示した図である。

【図１２】

図１１（ａ）に示すカード型デバイスの機能的構成を示した図である。

【符号の説明】

１　　カード型デバイス

１０　筐体

１１ａ　一端面（端面）

１３　接続端子

１４　信号処理部

１５　メモリ

１６　制御部

２　　指紋読取部

２１　光源

２１　回転ローラ

２１ａ　外周面

２２　光源

２３　セルフォックレンズアレイ

２４　基板

２５　一次元指紋読取センサ

３　　電子機器

３１　カード・スロット

３１ａ　接続コネクタ

６０　制御部

６３　プログラムメモリ

６３ａ　指紋照合プログラム

６３ｂ　声紋照合プログラム

６３ｃ　ユーザ認証プログラム

６４　データメモリ

６４ａ　指紋データ格納領域

６４ｂ　声紋データ格納領域

６５　Ｉ／Ｆ部

７　　カード型デバイス

７１　指紋照合プログラム格納領域

７２　指紋データ格納領域

８　　カード型デバイス

８１　暗号化回路

８２　秘密鍵メモリ

９　　カード型デバイス

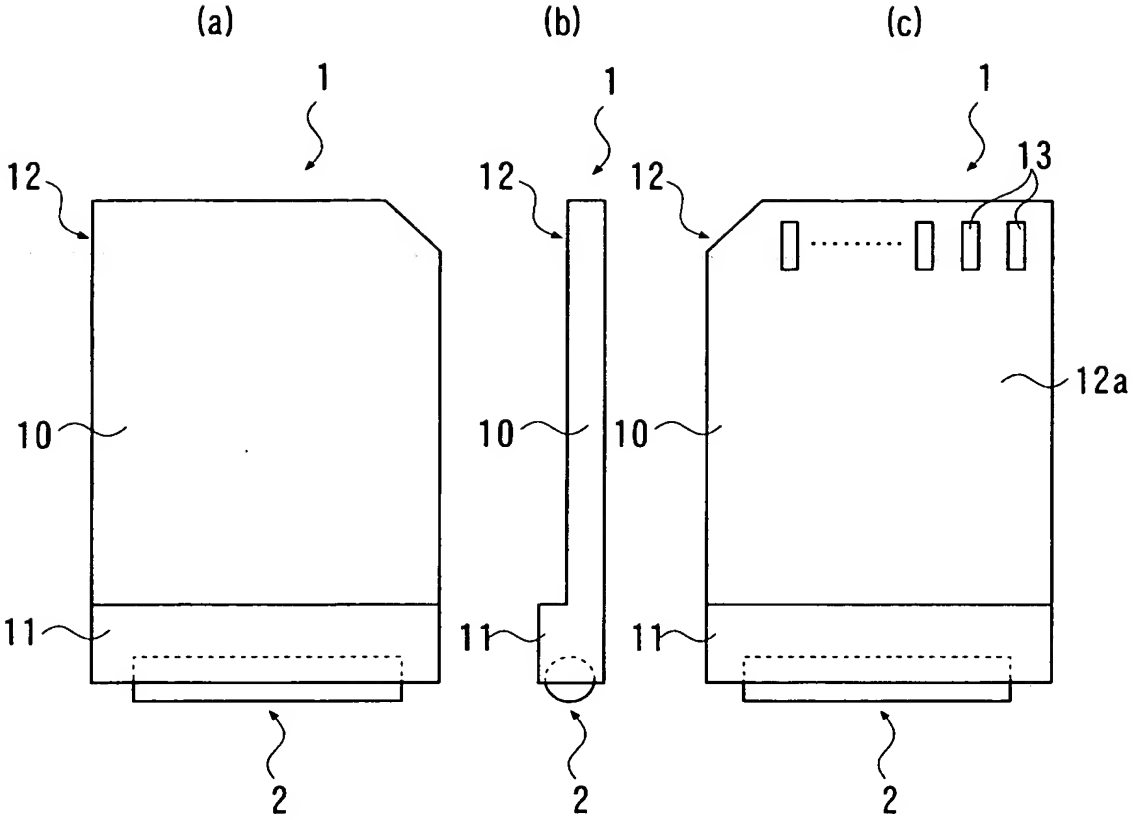
９２　ＵＳＢ接続端子

９３　ＵＳＢ入出力Ｉ／Ｆ回路

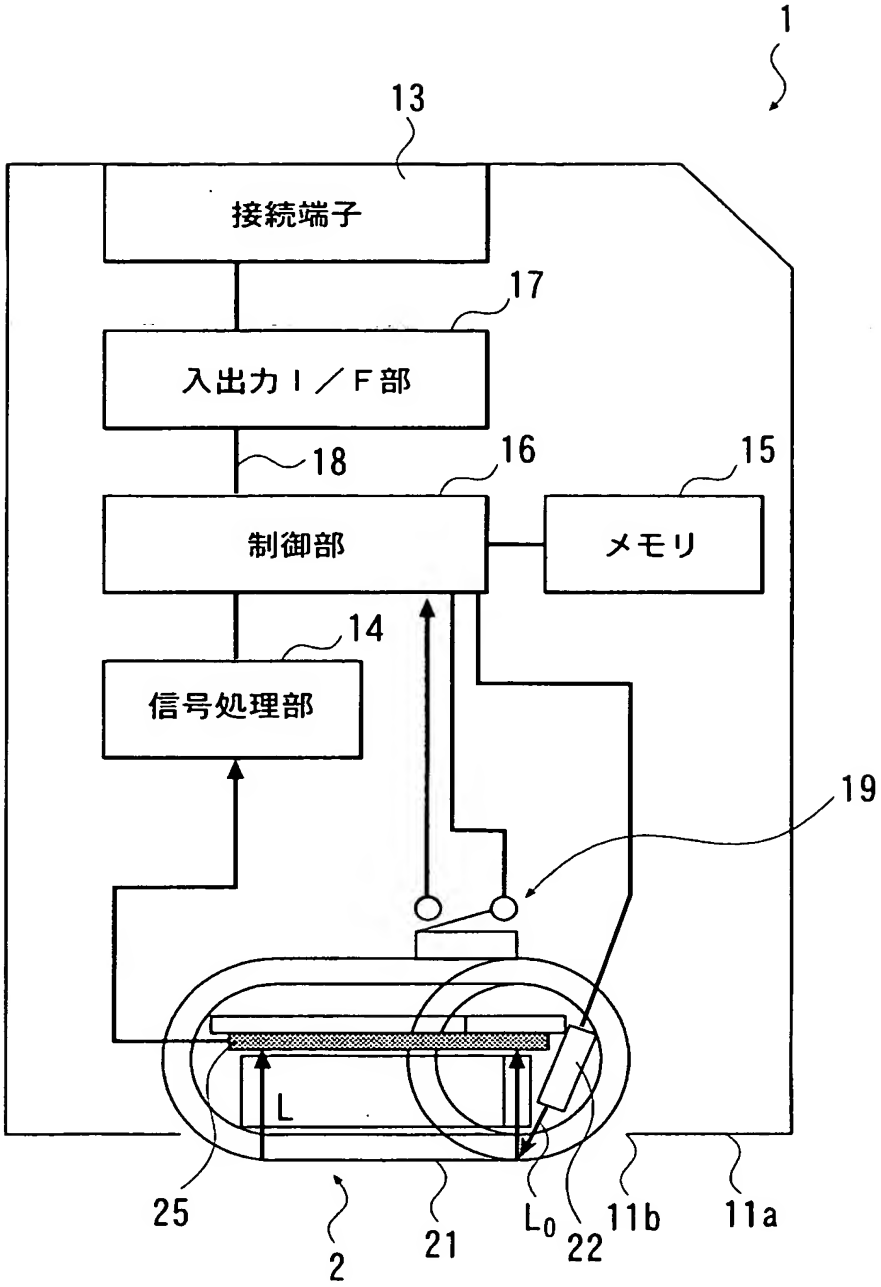
１００　指

【書類名】　　図面

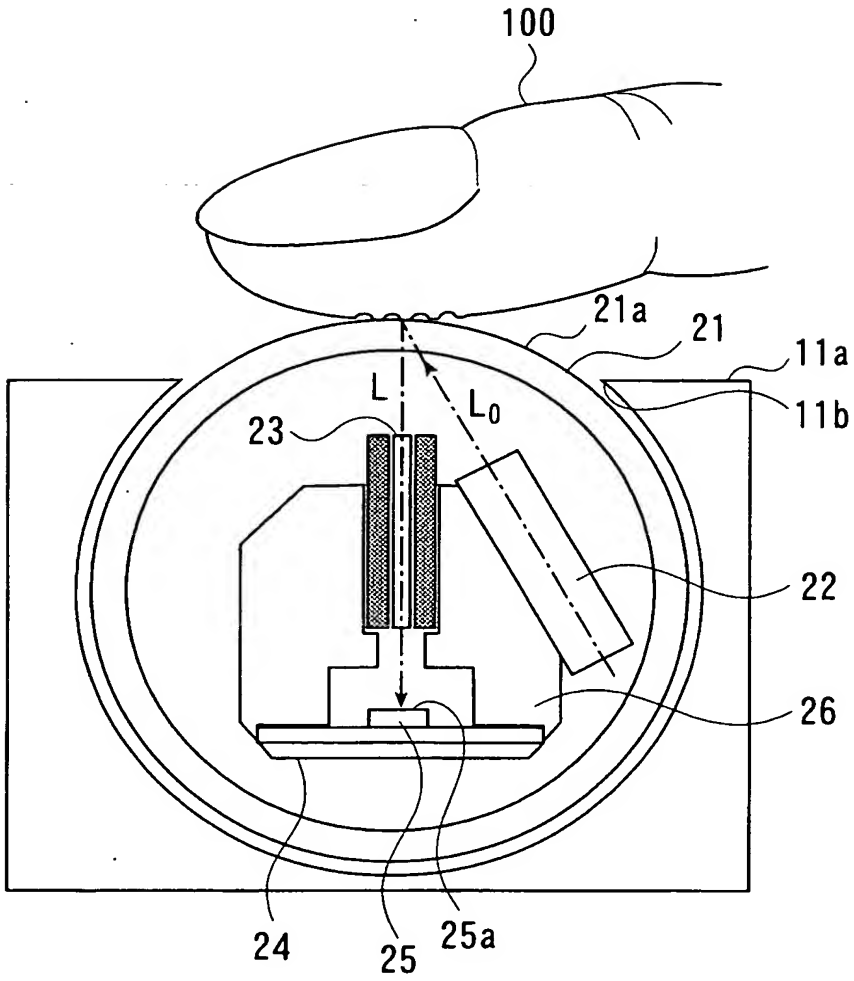
【図１】



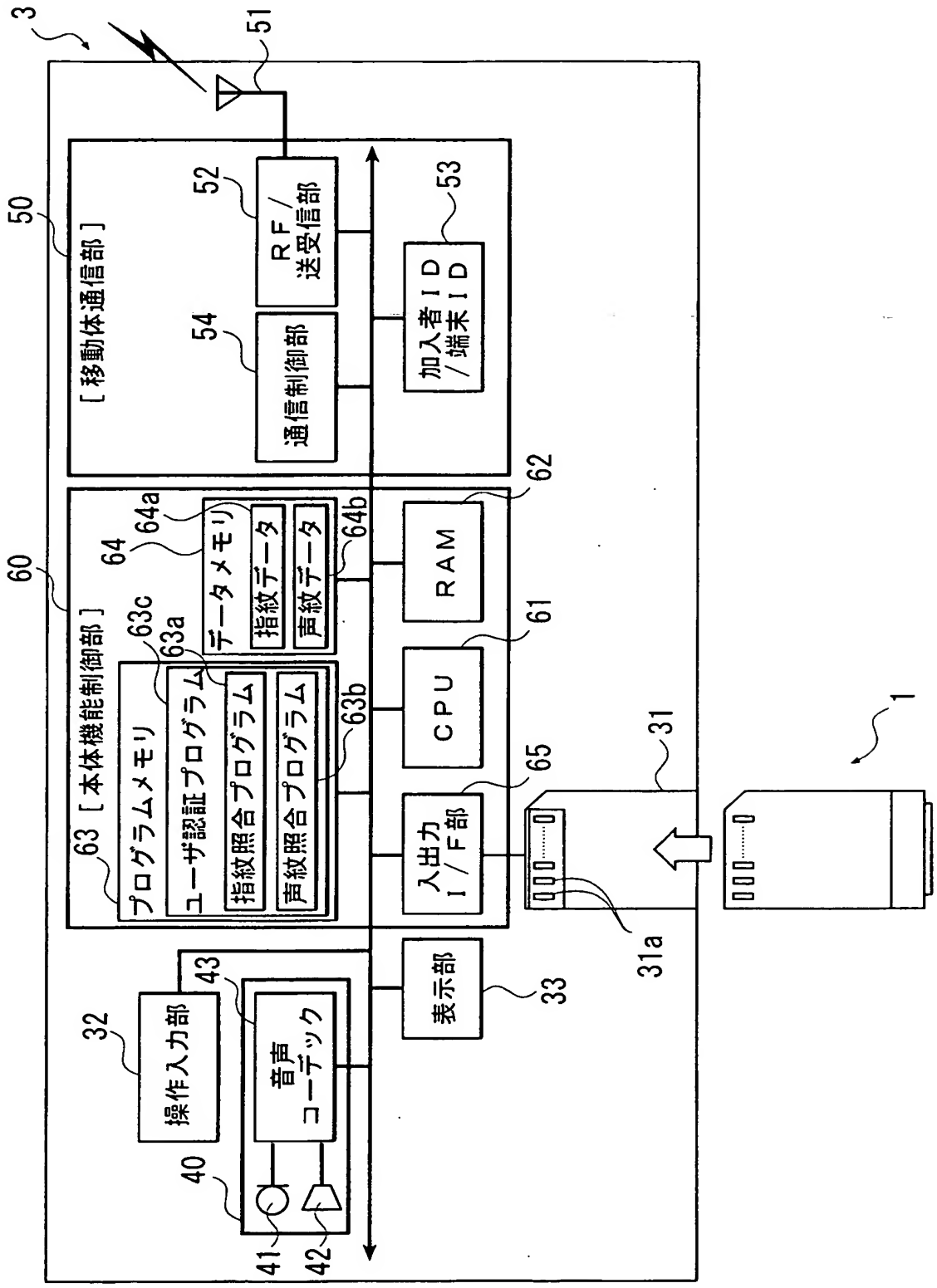
【図２】


1
13
接続端子
17
入出力Ｉ／Ｆ部
18
16
15
制御部
メモリ
14
信号処理部
19
L
25
2
21
L_0
22
11b
11a

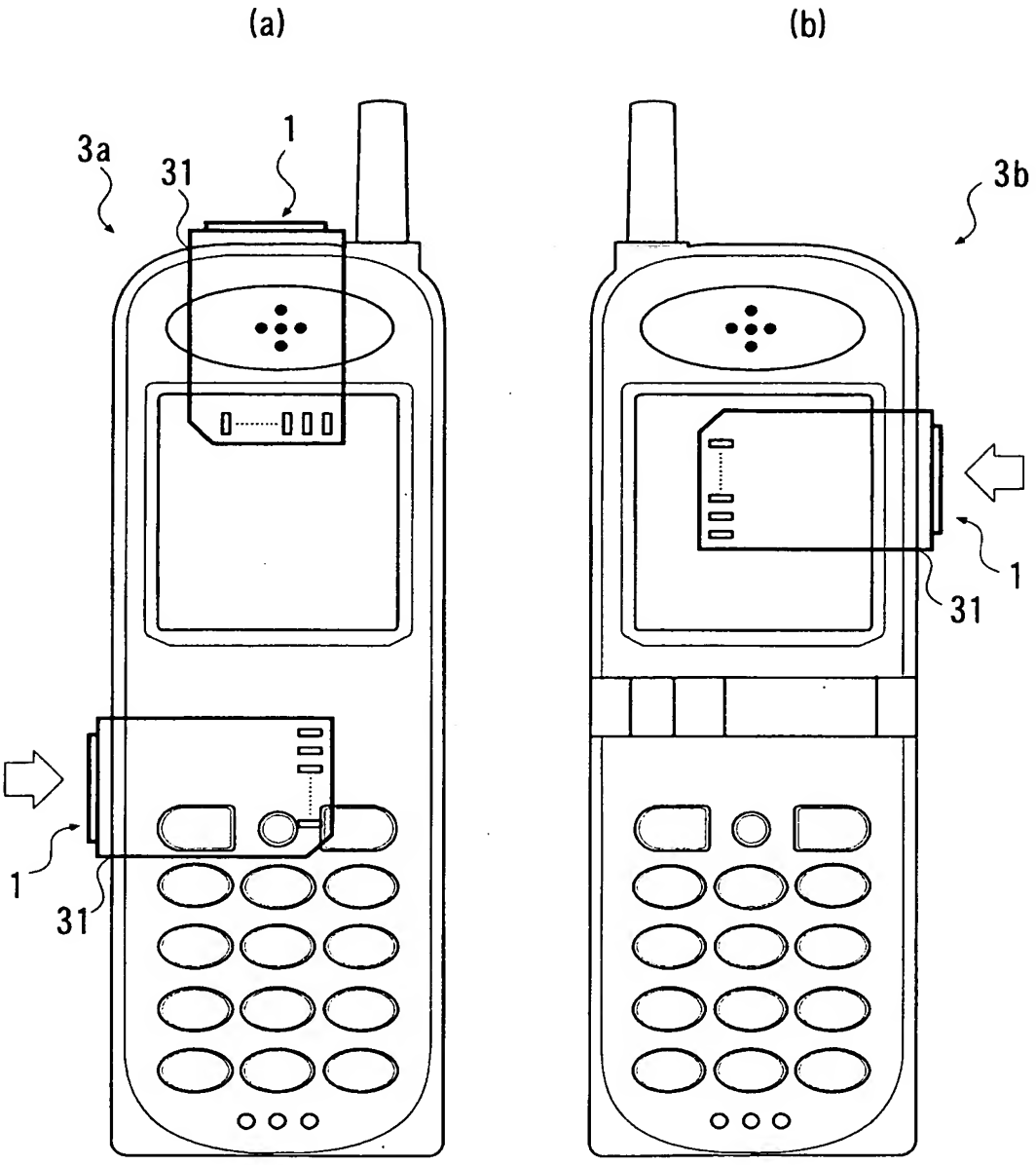
【図３】



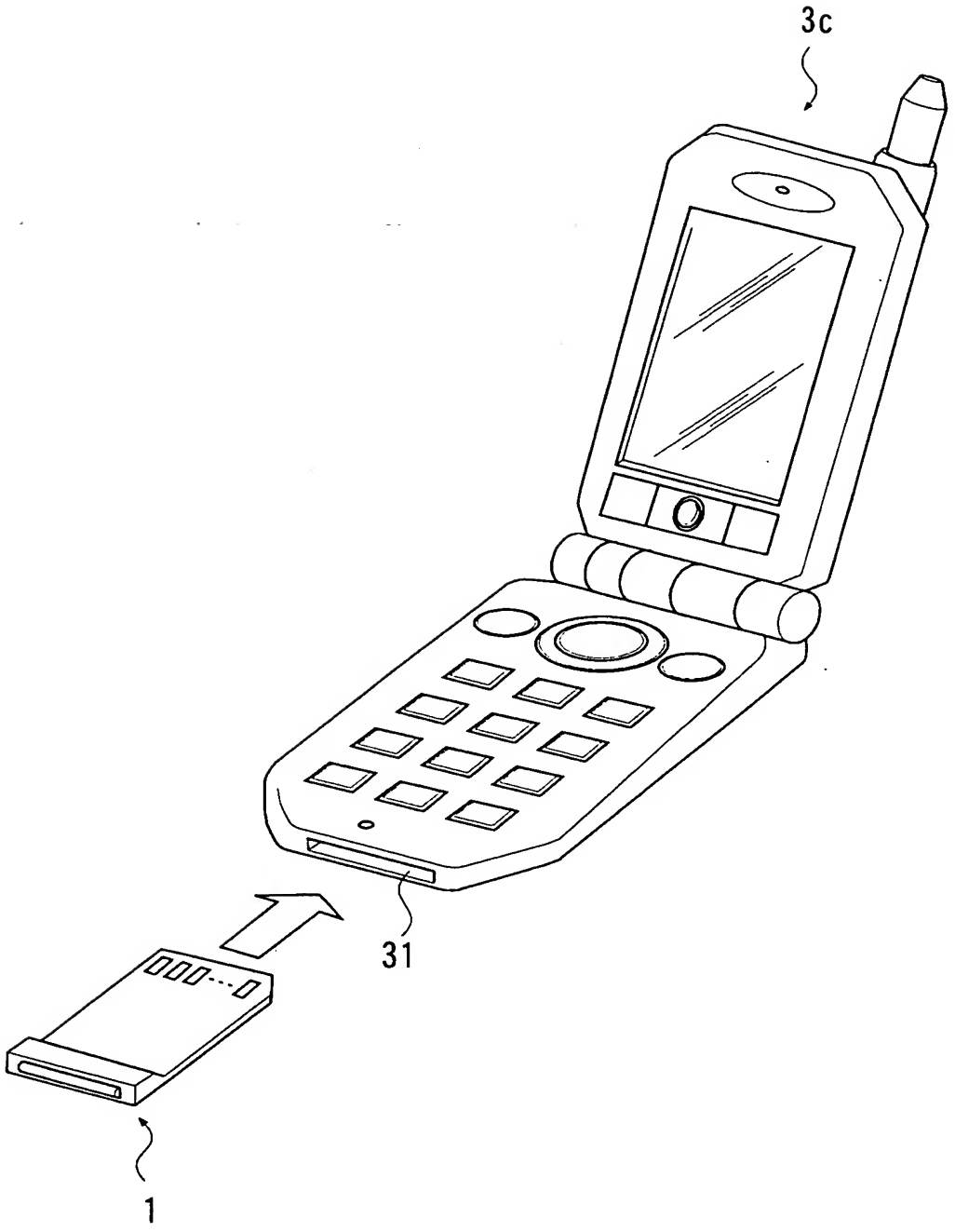
【図４】


3
51
50
［移動体通信部］
52
RF／送受信部
54
通信制御部
53
加入者ID／端末ID
60
［本体機能制御部］
64
64a
データメモリ
指紋データ
声紋データ
64b
62
RAM
63
［本体機能制御部］
プログラムメモリ
63c
63a
ユーザ認証プログラム
指紋照合プログラム
声紋照合プログラム
63b
61
CPU
65
入出力I／F部
31
1
31a
32
操作入力部
43
音声コーデック
40
41
42
表示部
33

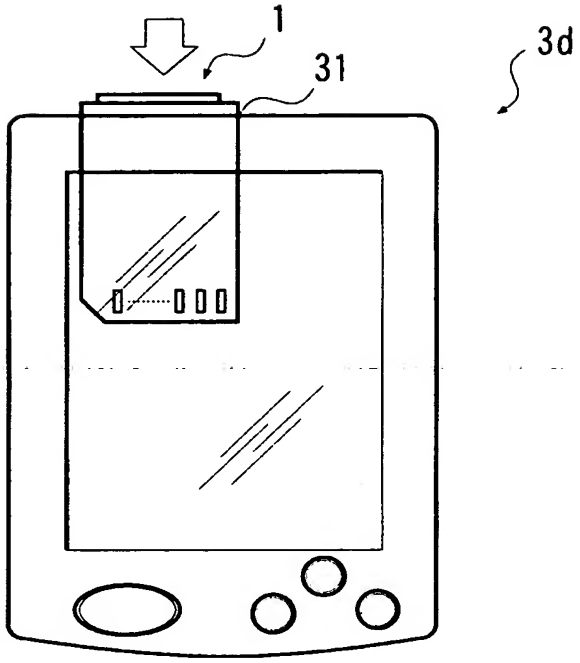
【図５】



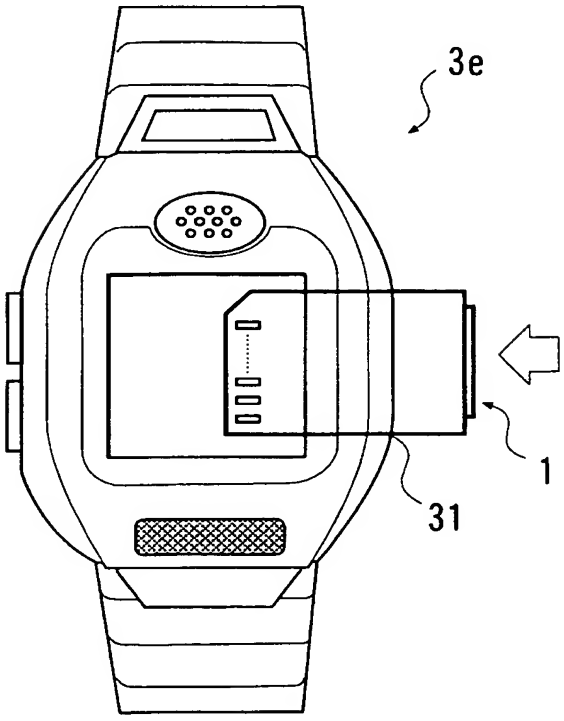
【図６】



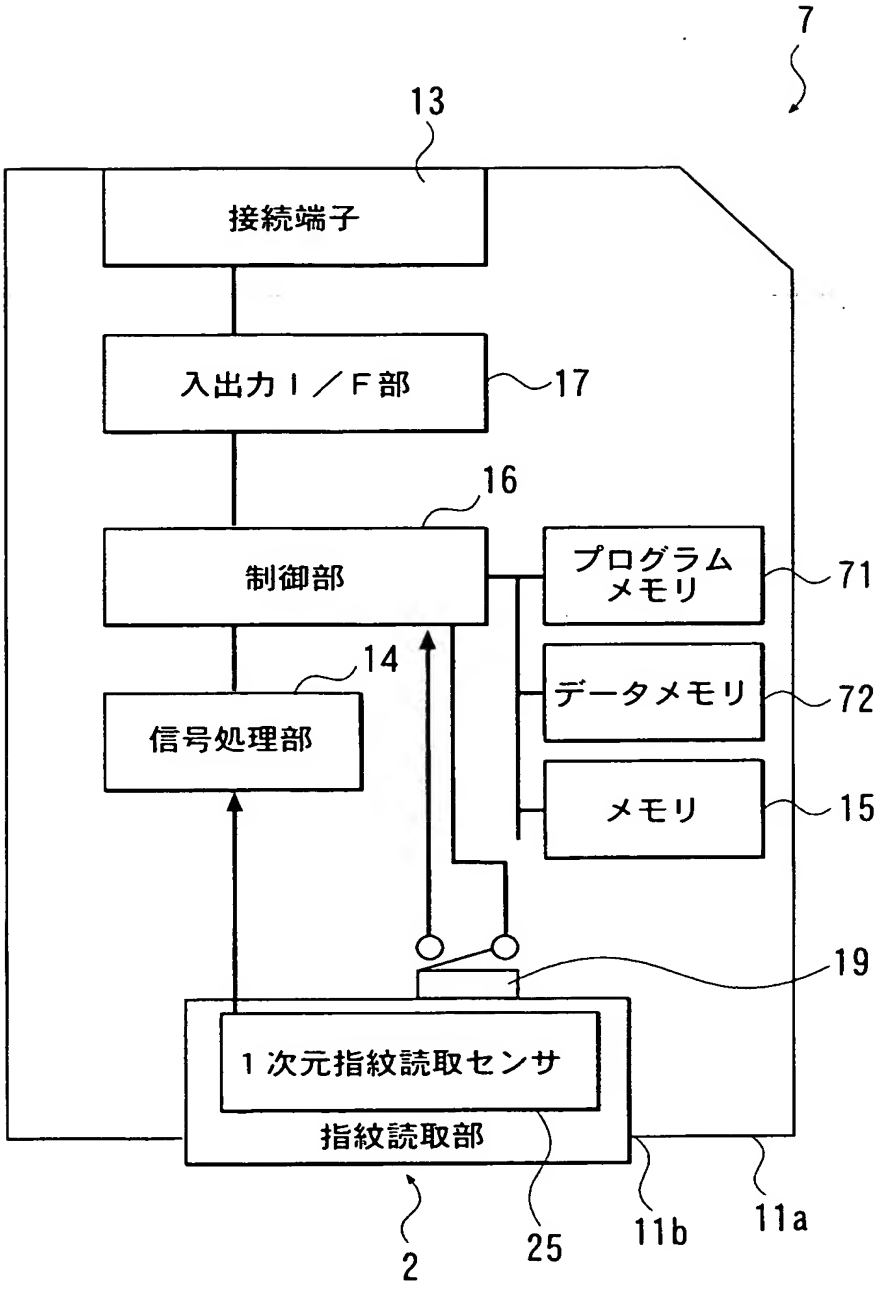
【図７】



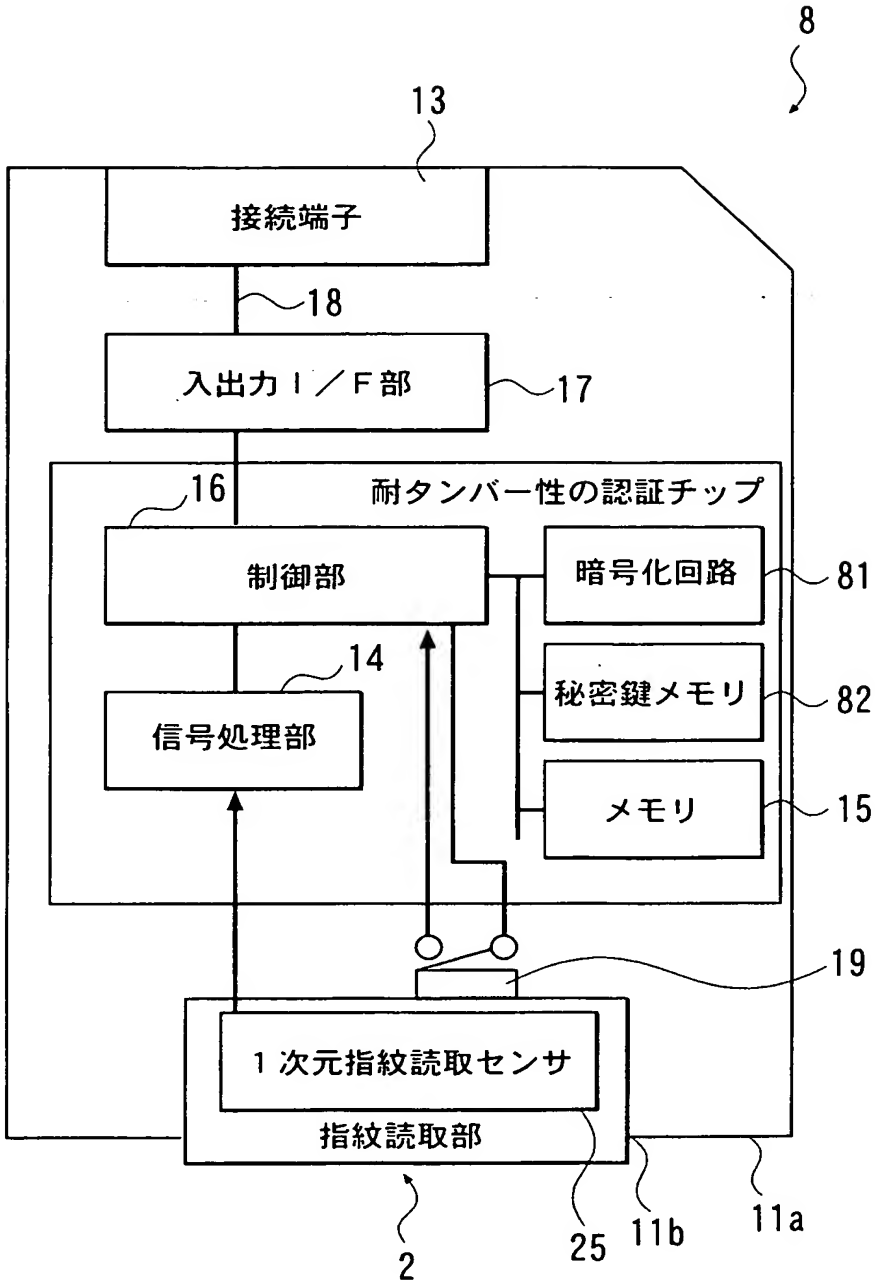
【図８】



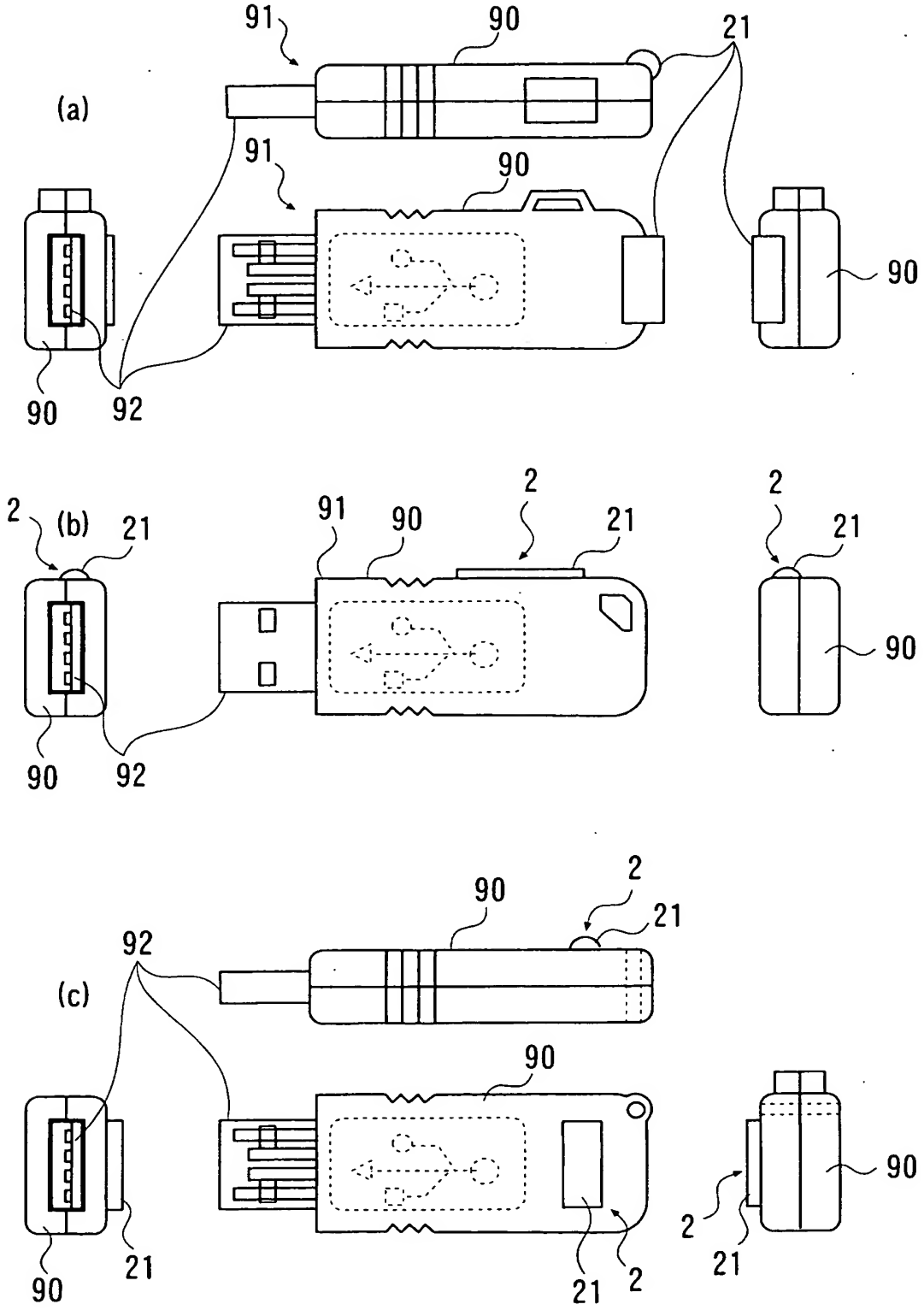
【図９】


7
13
接続端子
入出力Ｉ／Ｆ部
17
16
制御部
プログラムメモリ
71
14
信号処理部
データメモリ
72
メモリ
15
19
１次元指紋読取センサ
指紋読取部
2
25
11b
11a

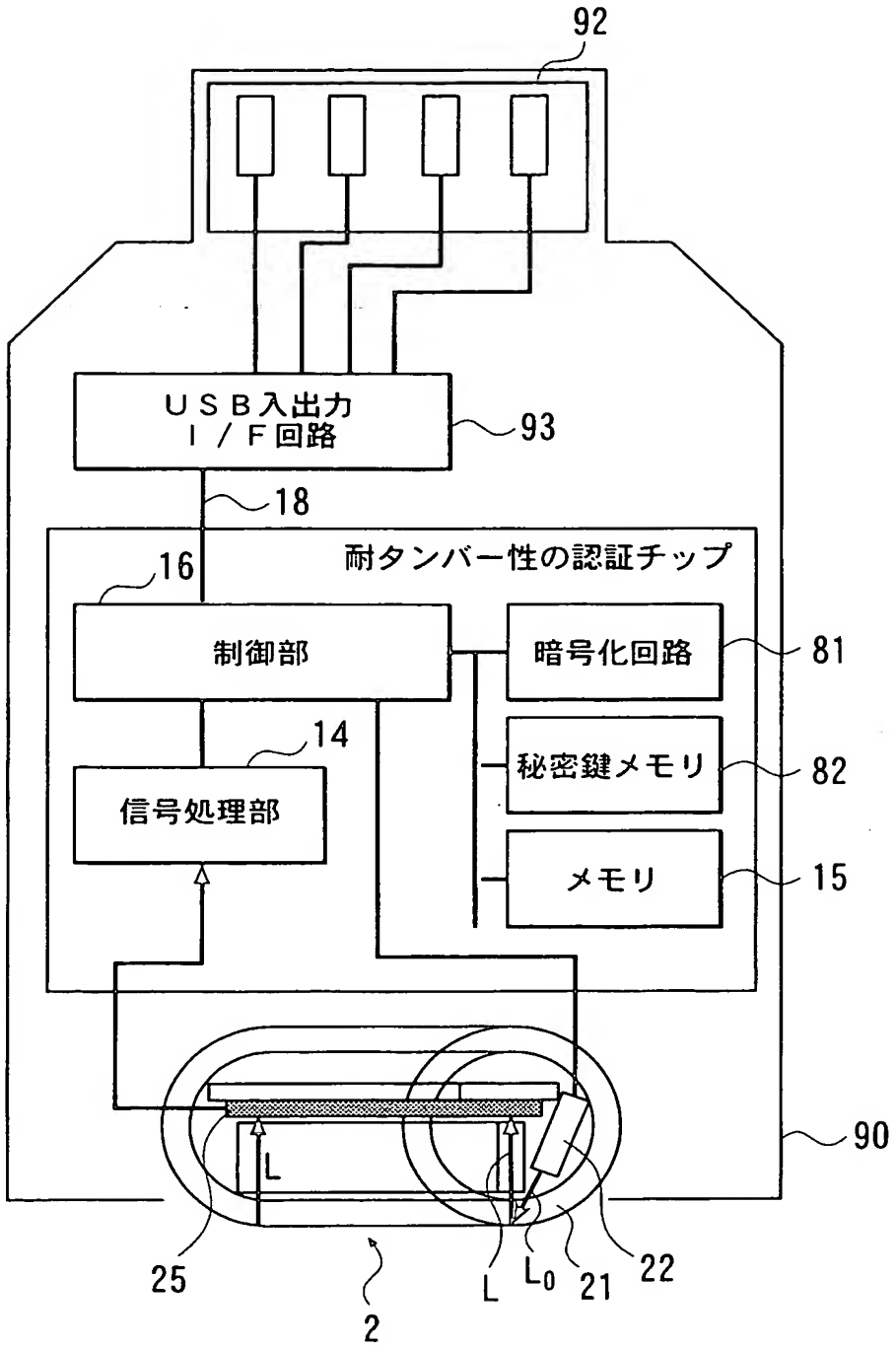
【図１０】


8
13
接続端子
18
入出力Ｉ／Ｆ部
17
16
耐タンパー性の認証チップ
制御部
暗号化回路
81
14
信号処理部
秘密鍵メモリ
82
メモリ
15
19
１次元指紋読取センサ
指紋読取部
2
25
11b
11a

【図１１】


(a)
91
90
21
91
90
90
90
92
(b)
2
21
91
90
2
21
2
21
90
90
92
(c)
92
90
2
21
90
90
21
90
2
21
21
2

【図１２】


92
ＵＳＢ入出力
Ｉ／Ｆ回路
93
18
耐タンパー性の認証チップ
16
制御部
暗号化回路
81
14
秘密鍵メモリ
82
信号処理部
メモリ
15
90
L
25
2
L
L_0
21
22

【書類名】　　要約書

【要約】

【課題】　指紋読取センサを搭載した超小型のカード型デバイスおよびこのカード型デバイスを用いた認証システムを提供する。

【解決手段】　接続端子１３を有するカード型の筐体１０の端面に、外周面２１ａが突出するように回転ローラ２１を設け、回転ローラ２１の外周面２１ａに当接される指１００の一次元指紋データを取得する一次元指紋データ取得部２５と、回転ローラ２１を回転させることにより、一次元指紋データ取得部２５により位置を連続的に変えて取得される一次元指紋データから二次元像としての指紋データを合成する指紋データ合成部１６と、電子機器３との間でデータの授受を行うインターフェース部１７を設ける。

【選択図】　　図２

特願２００２－３７４７２１

出　願　人　履　歴　情　報

識別番号　　［０００００１４４３］

１．変更年月日　　１９９８年　１月　９日
［変更理由］　　住所変更
住　所　　東京都渋谷区本町１丁目６番２号
氏　名　　カシオ計算機株式会社